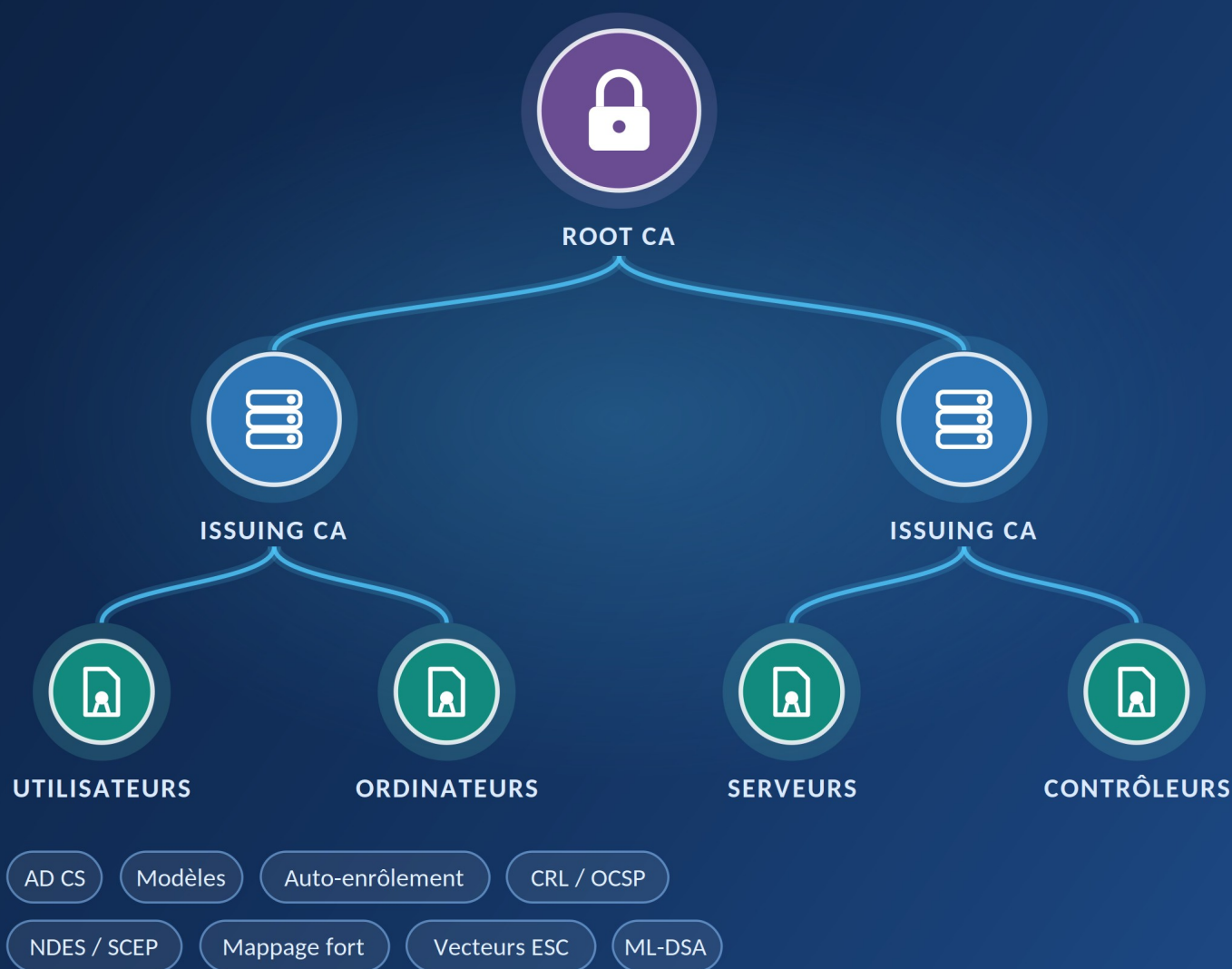


# Active Directory Certificate Services

Certificats, PKI et sécurité  
dans Active Directory



## Suivi du document

| Version | Date           | Évolutions                                                                                                                                                                                                                                                         |
|---------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.0     | Septembre 2026 | Refonte complète : 13 schémas vectoriels, corrections techniques (flux d'enrôlement, AIA/CDP en HTTP, OCSP), ajout du mappage fort (KB5014754), des vecteurs ESC1 à ESC16, des commandes de déploiement, de la publication AIA/CDP, de l'audit AD CS et de ML-DSA. |

## Sommaire

|                                                                      |           |
|----------------------------------------------------------------------|-----------|
| <b>1. Objectif et périmètre.....</b>                                 | <b>3</b>  |
| <b>2. Les bases : qu'est-ce qu'un certificat ?.....</b>              | <b>3</b>  |
| 2.1 Champs et extensions à connaître.....                            | 4         |
| <b>3. Usages des certificats dans Active Directory.....</b>          | <b>5</b>  |
| <b>4. Composants AD CS.....</b>                                      | <b>5</b>  |
| <b>5. Architecture de référence.....</b>                             | <b>6</b>  |
| <b>6. Hiérarchie PKI recommandée : deux niveaux.....</b>             | <b>6</b>  |
| 6.1 Mise en place de la racine hors ligne.....                       | 7         |
| 6.2 Mise en place d'une CA d'émission.....                           | 8         |
| <b>7. Chaîne de confiance et validation.....</b>                     | <b>8</b>  |
| 7.1 Distribution des certificats de CA.....                          | 9         |
| <b>8. Modèles de certificats.....</b>                                | <b>9</b>  |
| <b>9. Cycle d'émission d'un certificat.....</b>                      | <b>10</b> |
| <b>10. Auto-enrôlement par GPO.....</b>                              | <b>11</b> |
| <b>11. Exemple : certificat TLS serveur par auto-enrôlement.....</b> | <b>11</b> |
| <b>12. Révocation : CRL, delta CRL et OCSP.....</b>                  | <b>12</b> |
| <b>13. AIA et CDP.....</b>                                           | <b>13</b> |
| <b>14. NDES et SCEP.....</b>                                         | <b>14</b> |
| <b>15. CEP / CES : enrôlement via HTTPS.....</b>                     | <b>14</b> |
| <b>16. Certificats des contrôleurs de domaine.....</b>               | <b>15</b> |
| <b>17. Mappage fort des certificats (KB5014754).....</b>             | <b>15</b> |
| <b>18. Sécurité offensive AD CS : les vecteurs ESC.....</b>          | <b>16</b> |
| <b>19. Magasins de certificats Windows.....</b>                      | <b>17</b> |
| <b>20. Feuille de route de déploiement.....</b>                      | <b>17</b> |
| <b>21. Ports et dépendances réseau.....</b>                          | <b>18</b> |
| <b>22. Sécurité de la PKI.....</b>                                   | <b>18</b> |
| <b>23. Risques classiques et erreurs de conception.....</b>          | <b>19</b> |
| <b>24. Exploitation et supervision.....</b>                          | <b>19</b> |
| <b>25. Diagnostic : un certificat TLS n'est pas accepté.....</b>     | <b>20</b> |
| <b>26. Cycle de vie complet.....</b>                                 | <b>20</b> |
| <b>27. Exemple de matrice de modèles.....</b>                        | <b>21</b> |
| <b>28. Cryptographie moderne et post-quantique.....</b>              | <b>21</b> |
| <b>29. Checklist de recette avant production.....</b>                | <b>21</b> |
| <b>30. Références.....</b>                                           | <b>22</b> |
| <b>31. Glossaire.....</b>                                            | <b>22</b> |

## 1. Objectif et périmètre

Ce guide décrit le fonctionnement des certificats numériques dans un environnement Active Directory : principes cryptographiques, architecture d'une PKI Microsoft AD CS, émission, validation, renouvellement, révocation, utilisation par les applications, sécurisation et exploitation. Il s'appuie sur une architecture d'entreprise à deux niveaux : une autorité racine hors ligne et une ou plusieurs autorités d'émission intégrées à Active Directory.

**AD CS** (Active Directory Certificate Services) est le rôle Windows Server qui fournit l'infrastructure à clé publique (PKI) de l'entreprise. Une CA de type Enterprise s'appuie sur les modèles de certificats stockés dans AD DS ; ces modèles sont partagés par toutes les CA Enterprise de la forêt, ce qui garantit une application homogène de la politique de certification.

Le document s'adresse aux architectes, administrateurs Active Directory et PKI, ainsi qu'aux équipes sécurité. Les noms utilisés (contoso.com, pki.contoso.com, Contoso Root CA...) sont des exemples. Les durées, tailles de clé et périodes indiquées sont des valeurs de conception à adapter à la politique de certification de l'organisation.

## 2. Les bases : qu'est-ce qu'un certificat ?

Un certificat X.509 est un document numérique signé par une autorité de certification (CA). Il associe une identité (utilisateur, ordinateur, serveur, service ou équipement) à une clé publique. La clé privée correspondante reste sous le contrôle exclusif du titulaire : c'est la possession de cette clé qui prouve l'identité.

| Élément                        | Rôle                                                                                                                                                                 |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clé privée                     | Secret cryptographique du titulaire. Sert à signer ou à déchiffrer selon l'usage. Ne doit jamais être diffusée ; idéalement non exportable (TPM, carte à puce, HSM). |
| Clé publique                   | Diffusable. Permet de vérifier une signature du titulaire ou de chiffrer des données qu'il sera seul à pouvoir déchiffrer.                                           |
| Certificat                     | Lie l'identité à la clé publique : sujet, émetteur, validité, usages, extensions et signature de la CA.                                                              |
| Autorité de certification (CA) | Vérifie la demande selon sa politique et signe le certificat avec sa propre clé privée.                                                                              |
| Chaîne de confiance            | Enchaînement certificat final → CA intermédiaire(s) → racine présente dans le magasin des autorités racines approuvées.                                              |
| CRL / OCSP                     | Mécanismes permettant de savoir si un certificat a été révoqué avant son expiration.                                                                                 |

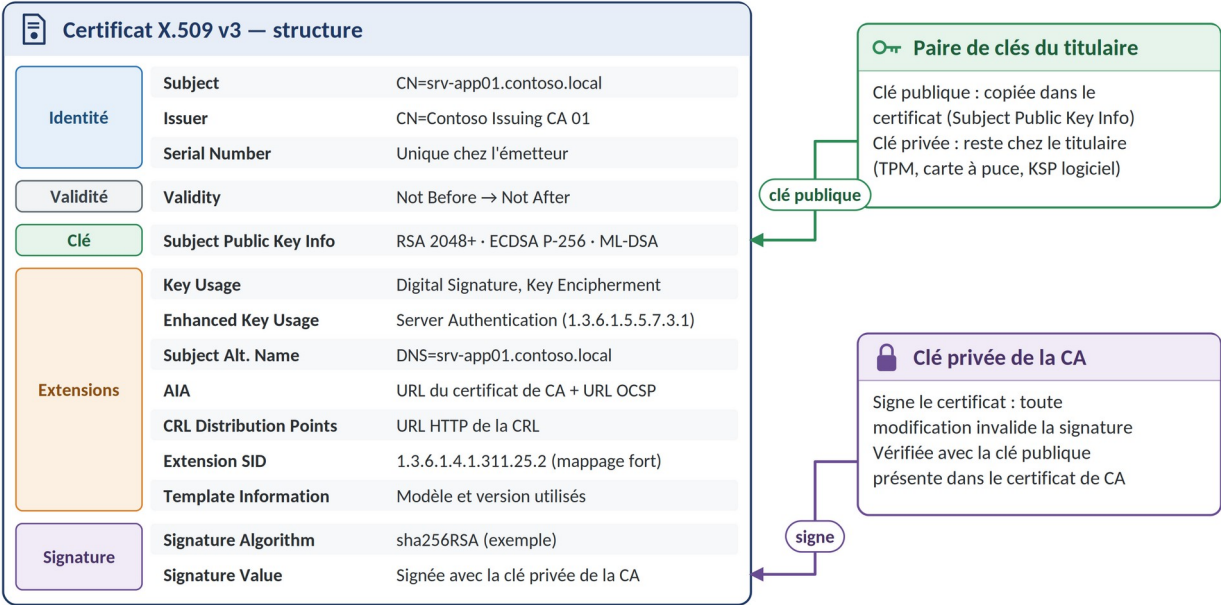


Figure 1 — Structure d'un certificat X.509 v3 et rôle des clés

2.1 Champs et extensions à connaître

| Champ / extension                  | Contenu et intérêt                                                                                                                       |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Subject                            | Identité principale portée par le certificat (nom distinctif).                                                                           |
| Issuer                             | Nom de la CA qui a signé le certificat.                                                                                                  |
| Serial Number                      | Identifiant unique chez l'émetteur ; c'est lui qui figure dans les CRL.                                                                  |
| Validity                           | Période de validité (Not Before / Not After).                                                                                            |
| Subject Public Key Info            | Clé publique et algorithme (RSA, ECDSA, ML-DSA).                                                                                         |
| Key Usage (KU)                     | Opérations cryptographiques autorisées : signature numérique, chiffrement de clé, signature de certificats...                            |
| Enhanced Key Usage (EKU)           | Usages applicatifs : Server Authentication, Client Authentication, Smart Card Logon, Code Signing, Secure Email...                       |
| Subject Alternative Name (SAN)     | Identités alternatives : noms DNS, UPN, adresse e-mail, URI. Les navigateurs et la plupart des applications TLS ne vérifient que le SAN. |
| Authority Information Access (AIA) | URL du certificat de la CA émettrice (construction de chaîne) et URL du répondeur OCSP.                                                  |
| CRL Distribution Points (CDP)      | URL de la liste de révocation à consulter.                                                                                               |
| Extension de sécurité SID          | OID 1.3.6.1.4.1.311.25.2 : SID du compte AD demandeur, ajouté par les CA Enterprise à jour ; base du mappage fort (section 17).          |

### 3. Usages des certificats dans Active Directory

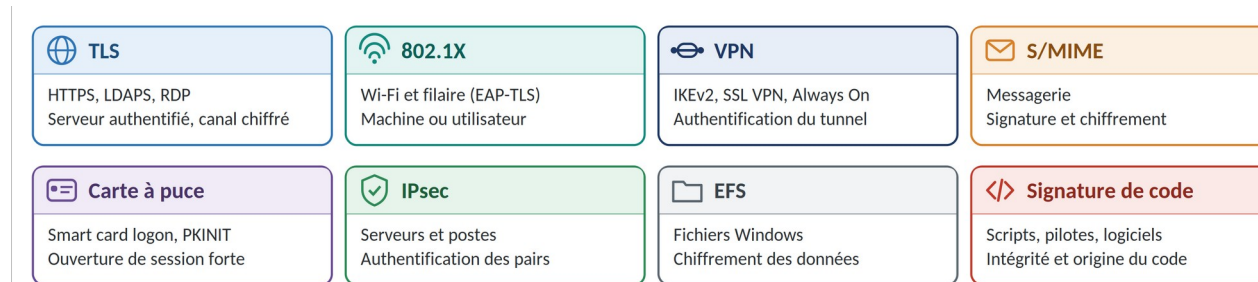


Figure 2 — Principaux usages des certificats émis par une PKI AD CS

| Cas d'usage            | Exemples                        | Fonction du certificat                                     |
|------------------------|---------------------------------|------------------------------------------------------------|
| TLS serveur            | IIS, LDAPS, RDP, applications   | Prouver l'identité du serveur et établir un canal chiffré. |
| TLS client / mTLS      | API, applications, proxys       | Authentifier le client par possession de la clé privée.    |
| 802.1X                 | Wi-Fi et filaire avec NPS       | Authentifier la machine ou l'utilisateur via EAP-TLS.      |
| VPN                    | IKEv2, Always On VPN, VPN tiers | Authentifier le client et/ou la passerelle du tunnel.      |
| Carte à puce           | Smart card logon, PKINIT        | Authentification forte auprès d'Active Directory.          |
| S/MIME                 | Messagerie                      | Signer et chiffrer les courriels.                          |
| EFS                    | Fichiers Windows                | Chiffrer des fichiers locaux.                              |
| IPsec                  | Serveurs et postes              | Authentifier les pairs et protéger les flux réseau.        |
| Signature de code      | Scripts PowerShell, logiciels   | Garantir l'origine et l'intégrité du code signé.           |
| Contrôleurs de domaine | Kerberos PKINIT, LDAPS          | Présenter l'identité cryptographique du DC (KDC).          |

### 4. Composants AD CS

| Composant                    | Fonction                                                                                                |
|------------------------------|---------------------------------------------------------------------------------------------------------|
| Certification Authority (CA) | Émet, renouvelle et révoque les certificats ; publie ses CRL.                                           |
| Enterprise CA                | CA intégrée à AD DS : utilise les modèles de certificats et les ACL AD, permet l'auto-enrôlement.       |
| Standalone CA                | CA indépendante d'AD ; adaptée à une racine hors ligne. Pas de modèles.                                 |
| Certificate Templates        | Politiques d'émission : identité, usages, cryptographie, durée, droits d'enrôlement.                    |
| Online Responder             | Répond aux requêtes OCSP sur l'état de révocation d'un certificat précis.                               |
| NDES                         | Registration Authority utilisant SCEP pour les équipements réseau et les terminaux gérés par MDM.       |
| CEP / CES                    | Services web de stratégie et d'enrôlement en HTTPS (clients hors domaine, autres forêts).               |
| CA Web Enrollment            | Pages web historiques /certsrv. À éviter : exposées en HTTP, elles sont la cible du relais NTLM (ESC8). |

## 5. Architecture de référence

La figure suivante présente les rôles et les flux d'une PKI AD CS d'entreprise. La racine hors ligne ne signe que les CA d'émission ; ces dernières traitent les demandes quotidiennes en s'appuyant sur Active Directory, et publient leurs CRL et certificats sur un point de publication HTTP consulté par toutes les parties qui valident des certificats.

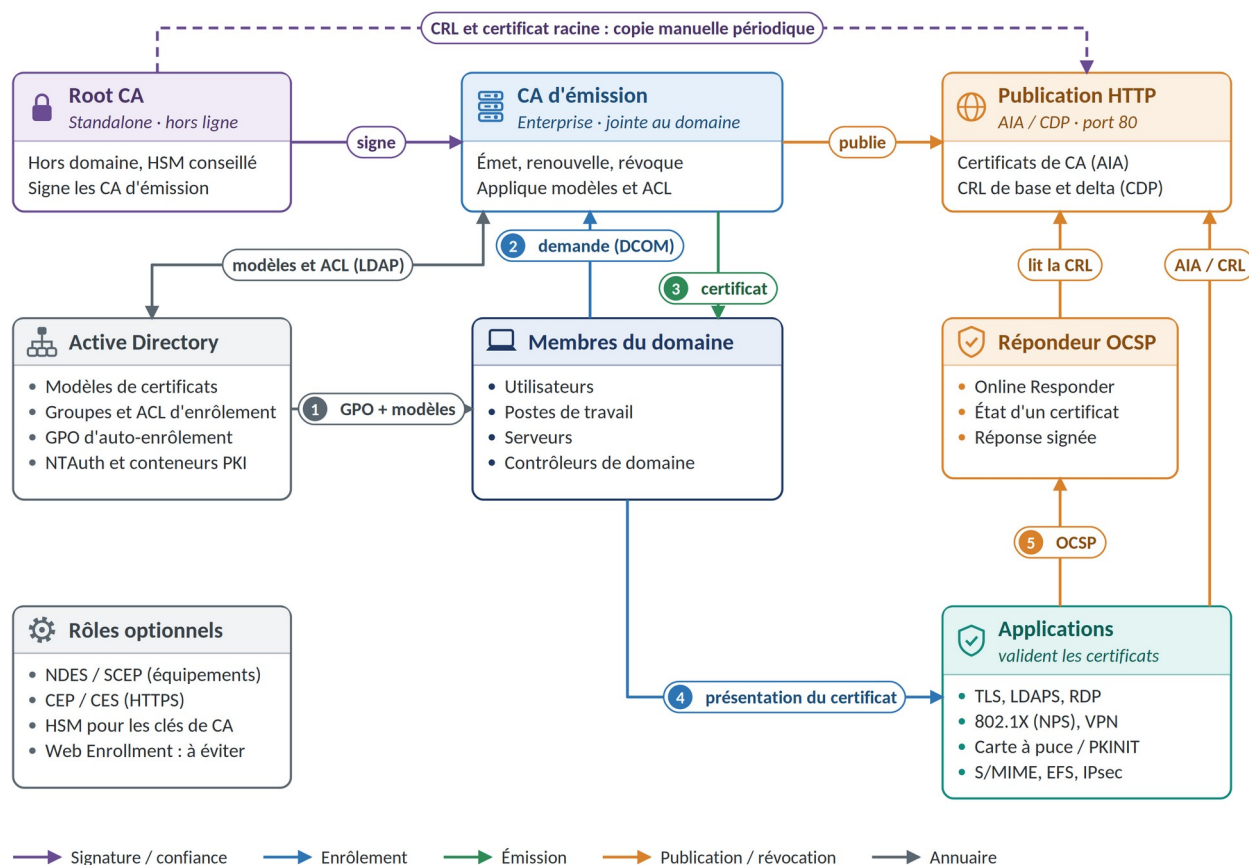


Figure 3 — Architecture de référence d'une PKI Microsoft AD CS à deux niveaux

- Découverte** : la GPO active l'auto-enrôlement ; le client lit dans AD les modèles auxquels il a droit et la liste des CA d'émission (LDAP).
- Demande** : le client génère sa paire de clés et envoie une requête PKCS#10 à la CA d'émission (DCOM/RPC, authentifiée Kerberos).
- Émission** : la CA vérifie l'ACL du modèle dans AD, construit le certificat, le signe et le renvoie.
- Présentation** : le titulaire présente son certificat à une application (TLS, EAP-TLS, PKINIT...).
- Validation** : l'application construit la chaîne (AIA) et vérifie la révocation (OCSP ou CRL) en HTTP.

### Attention

Les URL AIA et CDP doivent être publiées en **HTTP (port 80)** et non en HTTPS. Pour valider le certificat TLS d'un serveur HTTPS hébergeant la CRL, le client aurait besoin... de cette même CRL : la vérification tourne en boucle. Les CRL et réponses OCSP sont signées, leur intégrité ne dépend pas du transport.

## 6. Hiérarchie PKI recommandée : deux niveaux

La racine est isolée (hors domaine, éteinte ou déconnectée) et n'est utilisée que pour signer les certificats des CA d'émission et publier périodiquement sa CRL. Les CA d'émission, jointes au domaine, restent en ligne. Cette séparation réduit l'exposition de la clé racine : sa compromission imposerait de reconstruire toute la PKI.

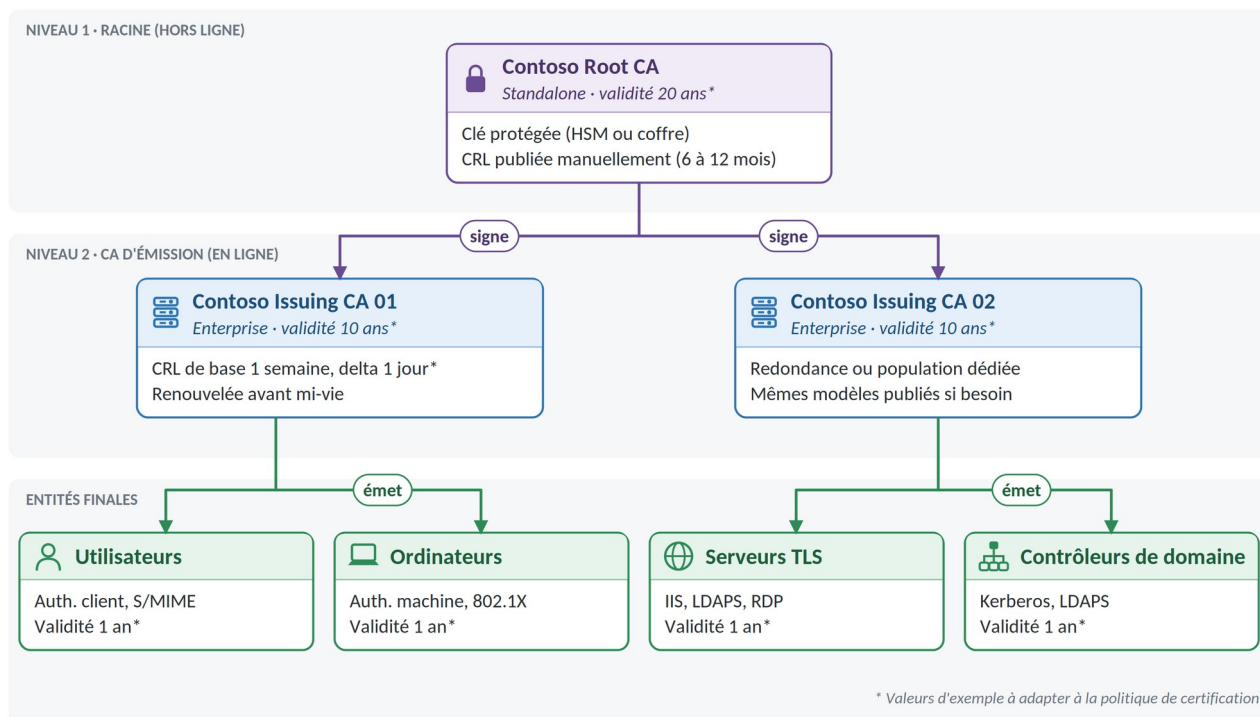


Figure 4 — Hiérarchie à deux niveaux : racine hors ligne, CA d'émission, entités finales

| Élément               | Valeur d'exemple             | Commentaire                                                                      |
|-----------------------|------------------------------|----------------------------------------------------------------------------------|
| Certificat Root CA    | 20 ans, RSA 4096             | Hors ligne, clé protégée par HSM ou procédure de coffre.                         |
| CRL de la Root CA     | 6 à 12 mois                  | Publication manuelle : rappel calendaire et recouvrement obligatoires.           |
| Certificat Issuing CA | 10 ans, RSA 2048 à 4096      | Renouveler avant la mi-vie pour pouvoir émettre des certificats de pleine durée. |
| CRL de l'Issuing CA   | Base 1 semaine, delta 1 jour | La delta CRL peut être supprimée si l'OCSP est déployé.                          |
| Certificats finaux    | 1 an ou moins                | Renouvelés automatiquement par auto-enrôlement.                                  |

Une CA ne peut pas émettre de certificat valide au-delà de sa propre date d'expiration : AD CS tronque la validité. Une hiérarchie à un seul niveau expose la clé racine en ligne ; une hiérarchie à trois niveaux (racine, CA de politique, CA d'émission) n'est justifiée que par des exigences réglementaires ou organisationnelles fortes.

## 6.1 Mise en place de la racine hors ligne

Le fichier `CAPolicy.inf` est placé dans `C:\Windows` avant l'installation du rôle. Exemple pour la racine :

```
[Version]
Signature="$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=Months
CRLPeriodUnits=12
CRLDeltaPeriodUnits=0
AlternateSignatureAlgorithm=0
```

```
# Installation de la racine autonome (serveur hors domaine)
Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
Install-AdcsCertificationAuthority -CAType StandaloneRootCA -CACommonName "Contoso Root CA" `
  -KeyLength 4096 -HashAlgorithmName SHA256 -ValidityPeriod Years -ValidityPeriodUnits 20 `
  -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"

# Durée des certificats de CA subordonnées (1 an par défaut sur une CA autonome)
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod "Years"
# Chemins LDAP corrects dans les extensions AIA/CDP
certutil -setreg CA\DSConfigDN "CN=Configuration,DC=contoso,DC=com"
Restart-Service certsvc ; certutil -crl
```

## 6.2 Mise en place d'une CA d'émission

Pour une CA Enterprise, ajouter `LoadDefaultTemplates=0` dans la section `[Certsrv_Server]` de son `CAPolicy.inf` afin de ne publier aucun modèle par défaut. La demande de certificat de CA est ensuite signée par la racine :

```
# Sur la CA d'émission (jointe au domaine, compte Enterprise Admins)
Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA `
  -CACommonName "Contoso Issuing CA 01" -KeyLength 4096 -HashAlgorithmName SHA256 `
  -OutputCertRequestFile C:\PKI\IssuingCA01.req

# Sur la racine : soumettre, approuver, récupérer
certreq -submit C:\PKI\IssuingCA01.req
certutil -resubmit <RequestId>
certreq -retrieve <RequestId> C:\PKI\IssuingCA01.crt

# Retour sur la CA d'émission (racine et CRL racine déjà publiées)
certutil -installcert C:\PKI\IssuingCA01.crt
Start-Service certsvc
```

## 7. Chaîne de confiance et validation

Lorsqu'un client reçoit un certificat, il ne se fie pas au nom affiché. Il construit une chaîne jusqu'à une racine présente dans son magasin des autorités racines approuvées, puis vérifie chaque maillon : signatures, dates, nom, usages, contraintes et, selon le contexte, état de révocation. Un seul échec suffit à rejeter le certificat.

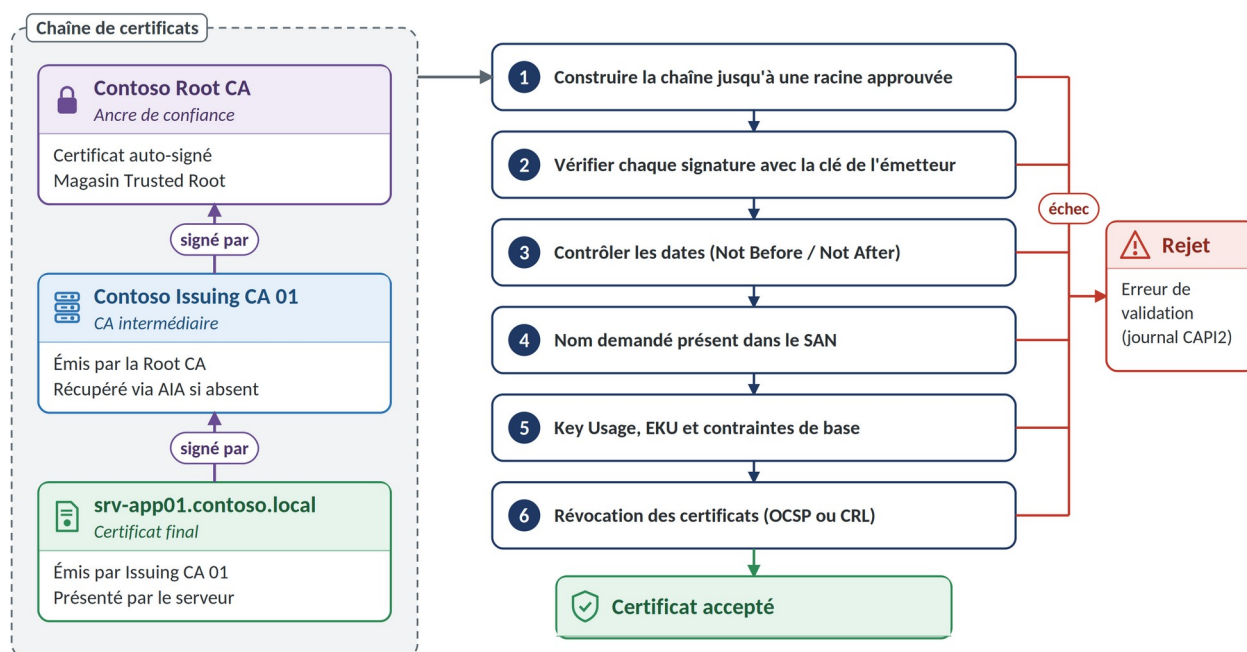


Figure 5 — Construction et validation d'une chaîne de certificats

## 7.1 Distribution des certificats de CA

Dans une forêt AD, la publication dans le conteneur Public Key Services suffit à distribuer automatiquement les certificats racine et intermédiaires aux membres du domaine. Une GPO (Public Key Policies > Trusted Root Certification Authorities) reste utile pour cibler finement ou pour les forêts approuvées.

```
# Publier la racine et sa CRL dans AD (depuis un poste du domaine)
certutil -dspublish -f ContosoRootCA.crt RootCA
certutil -dspublish -f ContosoRootCA.crl
# Contrôler le magasin NTAUTH de l'entreprise
certutil -viewstore -enterprise NTAUTH
```

Le magasin **NTAuth** liste les CA autorisées à émettre des certificats d'authentification AD (carte à puce, PKINIT). Une CA Enterprise y est ajoutée automatiquement à l'installation. Toute CA présente dans NTAUTH est un actif Tier 0 : un certificat d'authentification forgé par elle ouvre le domaine.

## 8. Modèles de certificats

Les modèles sont le cœur de l'automatisation d'une CA Enterprise. Stockés dans AD (**CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration**) et répliqués dans la forêt, ils ne sont émis par une CA qu'après avoir été ajoutés à ses modèles à délivrer.

| Paramètre        | Ce qu'il contrôle                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------|
| Compatibility    | Version du modèle et fonctions disponibles (v1 : non modifiable ; v2 : 2003 ; v3 : CNG ; v4 : 2012 et plus). |
| General          | Nom, durée de validité, période de renouvellement, publication dans AD.                                      |
| Request Handling | Objectif, exportabilité de la clé privée, archivage de clé.                                                  |
| Cryptography     | Fournisseur (KSP/CSP), algorithme, taille minimale de clé, hachage.                                          |
| Subject Name     | Identité construite depuis AD ou fournie dans la demande (« Supply in the request »).                        |

| Paramètre             | Ce qu'il contrôle                                                           |
|-----------------------|-----------------------------------------------------------------------------|
| Extensions            | Key Usage, Application Policies (EKU), Issuance Policies, contraintes.      |
| Security              | Qui peut Read, Enroll, Autoenroll et modifier le modèle.                    |
| Issuance Requirements | Approbation du gestionnaire de certificats, signatures autorisées requises. |
| Superseded Templates  | Remplacement progressif d'anciens modèles par auto-enrôlement.              |

### Attention

Ne jamais accorder Enroll ou Autoenroll plus largement que nécessaire, en particulier à Domain Users, Domain Computers ou Authenticated Users.

Un modèle qui combine « **Supply in the request** », un EKU d'authentification et un enrôlement ouvert sans approbation permet à n'importe quel utilisateur d'obtenir un certificat au nom d'un administrateur (ESC1, section 18).

## 9. Cycle d'émission d'un certificat

La paire de clés est générée par le client. Seule la clé publique, incluse dans la requête PKCS#10 signée, est transmise à la CA ; la CA renvoie le certificat signé, jamais de clé privée. La figure détaille les échanges d'un enrôlement AD CS standard.

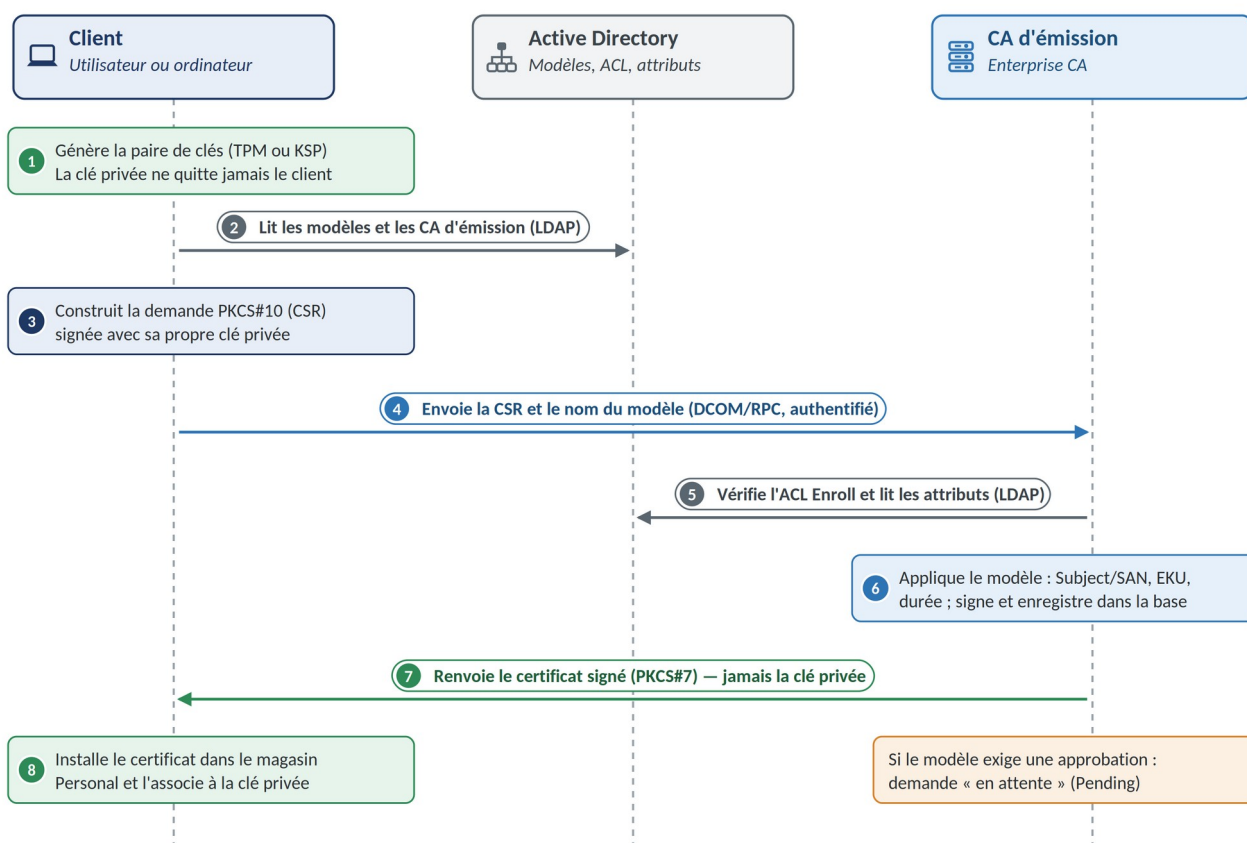


Figure 6 — Séquence d'enrôlement auprès d'une CA Enterprise

Exception : si le modèle impose l'**archivage de clé**, le client transmet aussi sa clé privée, chiffrée pour la CA, qui la conserve pour les agents de récupération de clé (KRA). Cette option n'est pertinente que pour les clés de chiffrement (EFS, S/MIME), jamais pour les clés de signature ou d'authentification.

## 10. Auto-enrôlement par GPO

L'auto-enrôlement permet aux utilisateurs et ordinateurs autorisés d'obtenir puis de renouveler automatiquement leurs certificats, sans intervention. Il se configure dans une GPO : Computer ou User Configuration > Politiques > Windows Settings > Security Settings > Public Key Policies > **Certificate Services Client – Auto-Enrollment**.

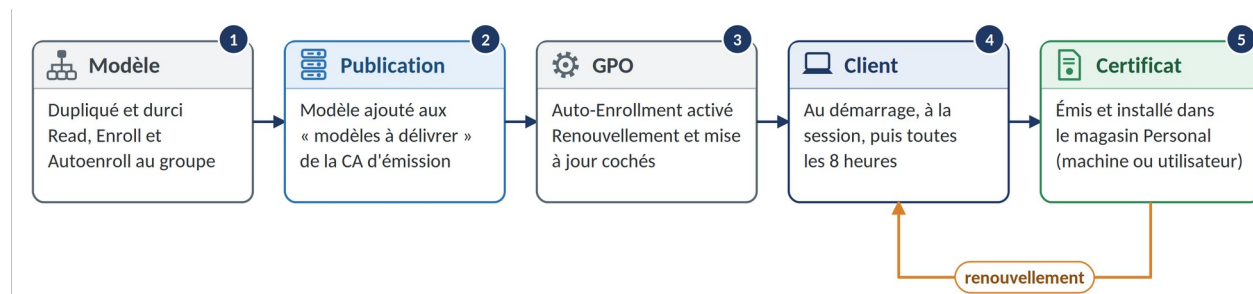


Figure 7 — Chaîne de mise en œuvre de l'auto-enrôlement

1. Dupliquer un modèle adapté (jamais modifier les modèles par défaut) et le passer en version 2 ou supérieure.
2. Configurer cryptographie, Subject/SAN construits depuis AD, EKU, durée et période de renouvellement.
3. Dans Security, accorder Read, Enroll et Autoenroll uniquement au groupe cible.
4. Publier le modèle sur la CA d'émission : Certificate Templates > New > Certificate Template to Issue.
5. Activer Auto-Enrollment dans une GPO liée aux OU concernées, avec « Renew expired certificates... » et « Update certificates that use certificate templates » cochés.
6. Actualiser les stratégies puis contrôler l'enrôlement.

Le client évalue l'auto-enrôlement au démarrage, à l'ouverture de session, lors du rafraîchissement des stratégies et toutes les 8 heures via les tâches planifiées `\Microsoft\Windows\CertificateServicesClient`. Il renouvelle un certificat dès que la période de renouvellement du modèle est atteinte.

```

gpupdate /force
certutil -pulse           # déclenche l'auto-enrôlement machine
certlm.msc               # magasin ordinateur
certmgr.msc              # magasin utilisateur

# Inventaire PowerShell du magasin machine
Get-ChildItem Cert:\LocalMachine\My |
  Select-Object Subject, Issuer, NotBefore, NotAfter, Thumbprint, HasPrivateKey
  
```

## 11. Exemple : certificat TLS serveur par auto-enrôlement

Objectif : doter automatiquement les serveurs applicatifs d'un certificat TLS à leur nom DNS. On crée un groupe AD **PKI-TLS-Servers**, on duplique le modèle Web Server en **Corp-Server-TLS**, puis on cible la GPO d'auto-enrôlement sur l'OU des serveurs.

| Onglet           | Réglage recommandé                                                                            |
|------------------|-----------------------------------------------------------------------------------------------|
| General          | Validité 1 an, période de renouvellement 6 semaines, nom Corp-Server-TLS.                     |
| Request Handling | Signature and encryption ; clé privée non exportable.                                         |
| Cryptography     | Key Storage Provider, RSA 2048 minimum (ou ECDSA P-256), SHA-256.                             |
| Subject Name     | Build from this Active Directory information ; format DNS name ; DNS name inclus dans le SAN. |

| Onglet     | Réglage recommandé                                                                          |
|------------|---------------------------------------------------------------------------------------------|
| Extensions | Application Policies : Server Authentication uniquement.                                    |
| Security   | PKI-TLS-Servers : Read, Enroll, Autoenroll. Aucun droit d'enrôlement pour Domain Computers. |

Construit depuis AD, le SAN ne contient que le nom DNS du serveur (`dNSHostName`). Pour des alias ou un nom de service partagé, utiliser un modèle distinct à émission contrôlée (approbation du gestionnaire), jamais un modèle auto-enrôlé avec « Supply in the request ».

## 12. Révocation : CRL, delta CRL et OCSP

Un certificat encore valide dans le temps peut ne plus devoir être accepté : compromission de clé, départ d'un utilisateur, remplacement d'un serveur, erreur d'émission. La CA inscrit alors son numéro de série et le motif de révocation dans sa base, puis le publie dans la CRL suivante.

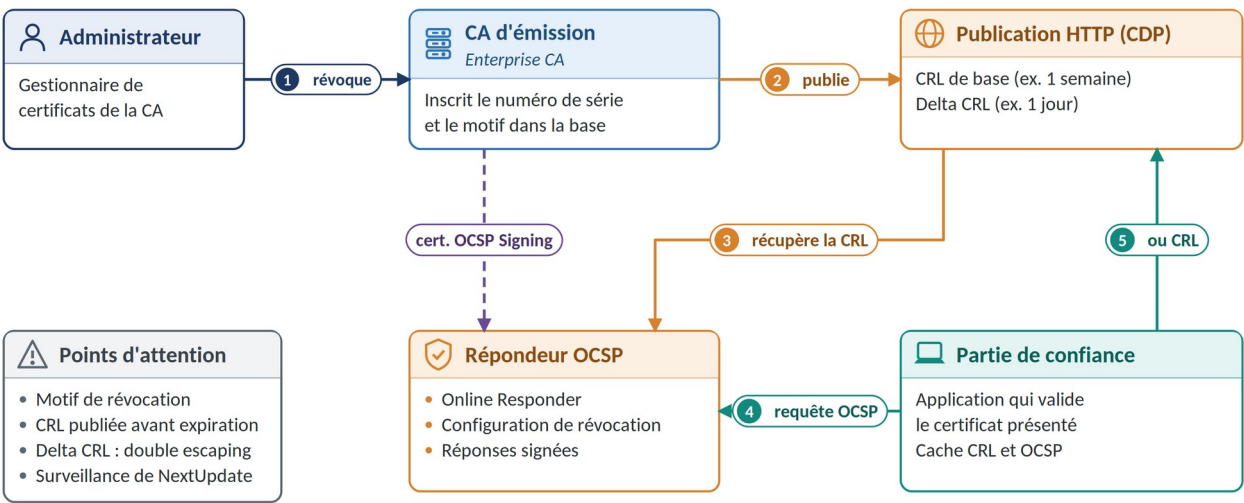


Figure 8 — Chaîne de révocation : de la décision à la vérification par l'application

| Mécanisme   | Principe                                                             | Points d'attention                                                                       |
|-------------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| CRL de base | Fichier signé listant tous les certificats révoqués non expirés.     | Doit être republiée avant son NextUpdate ; taille croissante.                            |
| Delta CRL   | Liste des révocations depuis la dernière CRL de base.                | Réduit le délai de prise en compte ; le « + » du nom impose le double escaping sous IIS. |
| OCSP        | Réponse signée sur l'état d'un certificat précis (Online Responder). | Certificat OCSP Response Signing à renouveler ; haute disponibilité nécessaire.          |

```
# Révoquer un certificat (motif 1 = compromission de clé)
certutil -revoke <NumeroDeSerie> 1
# Publier immédiatement une nouvelle CRL
certutil -crl
# Périodes de publication de la CA d'émission
certutil -setreg CA\CRLPeriodUnits 1
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 1
certutil -setreg CA\CRLDeltaPeriod "Days"
Restart-Service certsvc
```

Le motif « Certificate Hold » est le seul réversible. Les clients mettent en cache CRL et réponses OCSP : une révocation n'est visible qu'après expiration du cache ou publication d'une nouvelle CRL, d'où l'intérêt d'une delta CRL courte ou de l'OCSP.

## 13. AIA et CDP

Les extensions AIA et CDP sont inscrites dans chaque certificat émis et y restent jusqu'à son expiration. Elles doivent donc être conçues **avant** l'émission du premier certificat, sur des URL HTTP stables, hautement disponibles et accessibles depuis toutes les zones où les certificats sont validés.

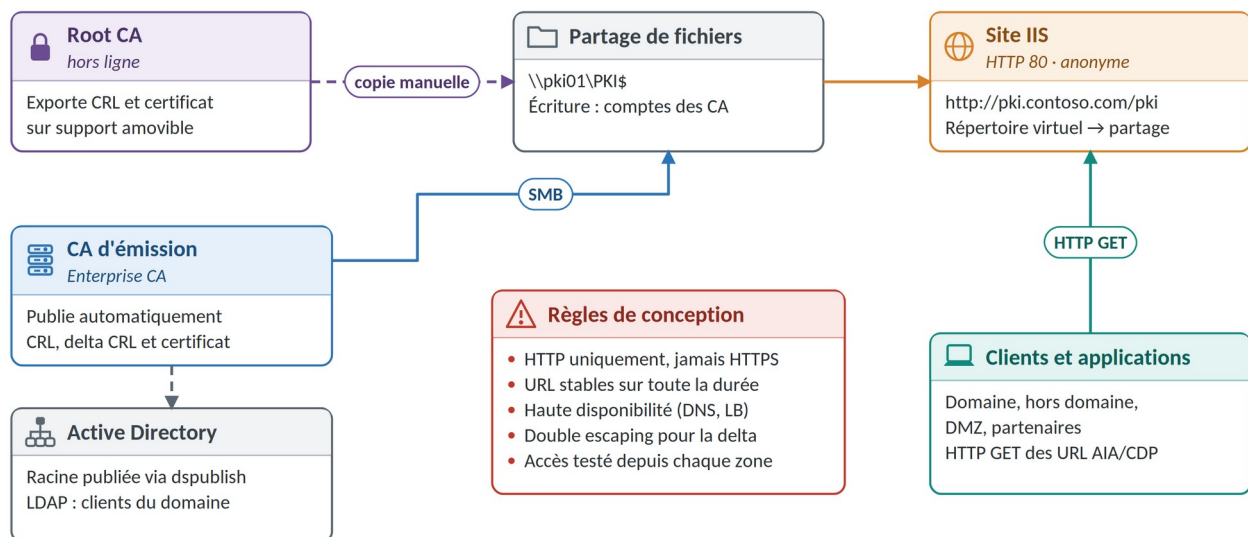


Figure 9 — Publication des certificats de CA et des CRL

```

# Sur la CA d'émission : remplacer les emplacements par défaut
Get-CACrLDistributionPoint | Remove-CACrLDistributionPoint -Force
$crl = '<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl'
Add-CACrLDistributionPoint -Uri "C:\Windows\System32\CertSrv\CertEnroll\$crl" `
    -PublishToServer -PublishDeltaToServer -Force
Add-CACrLDistributionPoint -Uri "file://\\pki01\PKI\$crl" `
    -PublishToServer -PublishDeltaToServer -Force
Add-CACrLDistributionPoint -Uri "http://pki.contoso.com/pki/$crl" `
    -AddToCertificateCdp -AddToFreshestCrl -Force

Get-CAAuthorityInformationAccess |
    Where-Object { $_.Uri -like 'ldap*' -or $_.Uri -like 'http*' } |
    Remove-CAAuthorityInformationAccess -Force
Add-CAAuthorityInformationAccess `
    -Uri 'http://pki.contoso.com/pki/<ServerDNSName>_<CAName><CertificateName>.crt' `
    -AddToCertificateAia -Force
Add-CAAuthorityInformationAccess -Uri 'http://ocsp.contoso.com/ocsp' -AddToCertificateOcsp -Force
Restart-Service certsrv ; certutil -crl

# Sur le serveur IIS (invite cmd) : autoriser le '+' des noms de delta CRL
%windir%\system32\inetsrv\appcmd set config "Default Web Site/pki" ^
    -section:system.webServer/security/requestFiltering -allowDoubleEscaping:true
  
```

Le compte ordinateur de chaque CA doit pouvoir écrire dans le partage. Les URL LDAP ne fonctionnent que pour les clients du domaine : dans une architecture moderne, on privilégie des URL HTTP seules. La console `pkiview.msc` (Enterprise PKI) vérifie l'accessibilité et l'expiration de chaque emplacement.

## 14. NDES et SCEP

NDES (Network Device Enrollment Service) joue le rôle de Registration Authority : il permet à des équipements qui ne parlent pas les protocoles d' enrôlement Microsoft (routeurs, commutateurs, terminaux mobiles, IoT) d' obtenir un certificat via SCEP. C' est aussi le socle des profils de certificats SCEP de Microsoft Intune, avec le connecteur de certificats Intune.

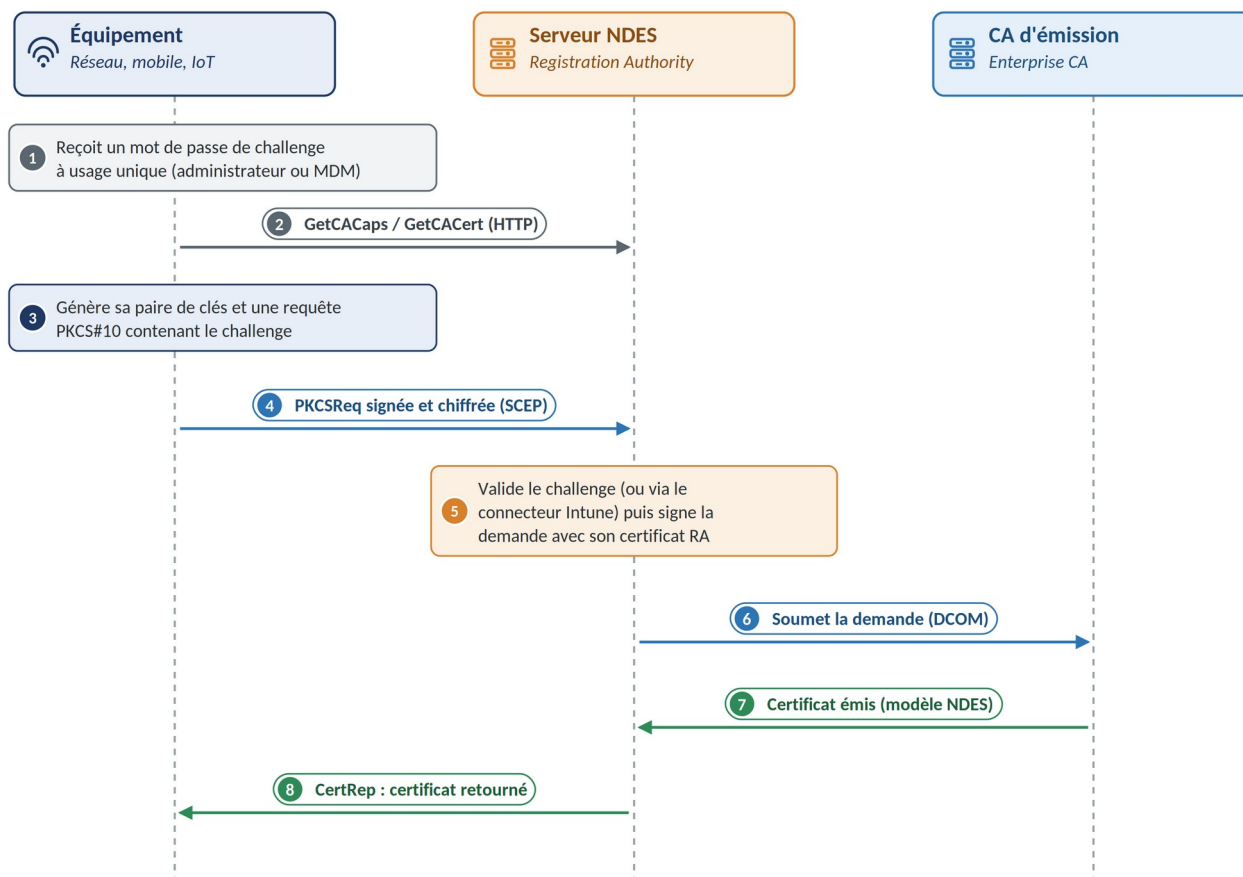
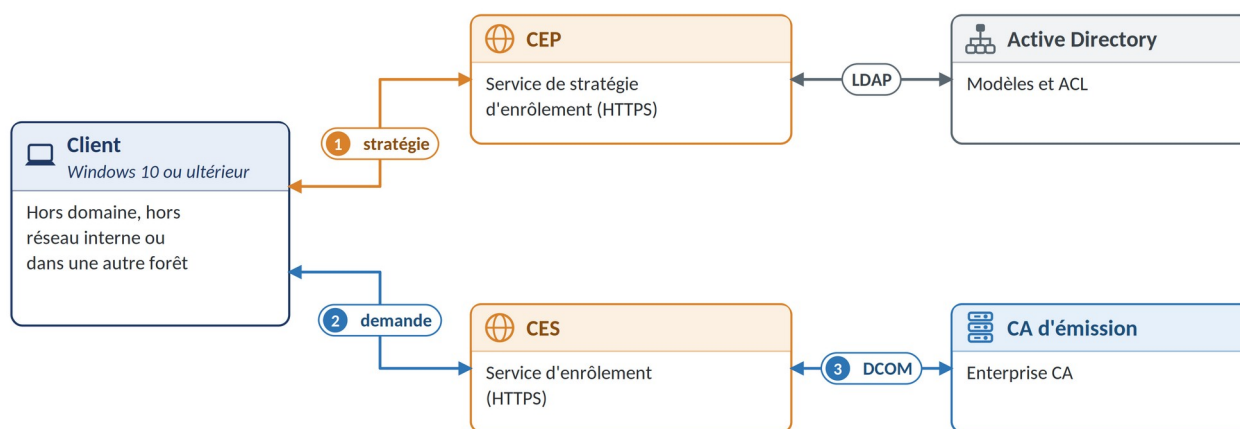


Figure 10 — Enrôlement SCEP via NDES

- Exécuter NDES sous un compte de service dédié disposant uniquement de Read et Enroll sur les modèles NDES.
- Le modèle émis est défini dans `HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP` (valeurs `EncryptionTemplate`, `GeneralPurposeTemplate`, `SignatureTemplate`).
- Surveiller l'expiration des certificats RA de NDES (Exchange Enrollment Agent et CEP Encryption) : leur expiration bloque tout enrôlement.
- Ne publier NDES sur Internet qu'au travers d'un reverse proxy ou d'un proxy d'application, jamais directement.
- Pour les certificats Intune utilisés en authentification AD, ajouter le SID de l'utilisateur ou de l'appareil dans le SAN (URI) afin de satisfaire le mappage fort.

## 15. CEP / CES : enrôlement via HTTPS

Le Certificate Enrollment Policy Web Service (**CEP**) expose la stratégie d' enrôlement ; le Certificate Enrollment Web Service (**CES**) transporte les demandes et les certificats en HTTPS, puis contacte la CA en DCOM pour le compte du demandeur. Ce couple sert les machines hors domaine, hors réseau interne ou situées dans une autre forêt, et permet de consolider les CA de plusieurs forêts.



Authentification au choix : Kerberos (intégrée), nom d'utilisateur et mot de passe, ou certificat client (renouvellement par clé).

Figure 11 — Enrôlement par les services web CEP et CES

Si CES est installé, activer la protection étendue de l'authentification (EPA) et exiger HTTPS : un CES accessible en NTLM sans EPA est vulnérable au relais NTLM, comme Web Enrollment.

## 16. Certificats des contrôleurs de domaine

Les contrôleurs de domaine utilisent des certificats pour LDAPS et pour le rôle KDC dans l'authentification par carte à puce et PKINIT. Il est recommandé de gérer explicitement leur modèle plutôt que de laisser coexister d'anciens certificats.

- Publier le modèle **Kerberos Authentication** (ou une copie) et le déclarer comme remplaçant de Domain Controller et Domain Controller Authentication (onglet Superseded Templates).
- Cibler une GPO d'auto-enrôlement sur l'OU Domain Controllers.
- Vérifier ECU (KDC Authentication, Server Authentication, Client Authentication, Smart Card Logon), SAN (FQDN du DC et du domaine) et accès aux CRL.
- Contrôler les certificats présents dans Local Computer\Personal et leur utilisation effective avant toute suppression.

## 17. Mappage fort des certificats (KB5014754)

Historiquement, un DC associait un certificat à un compte à partir du seul UPN ou nom DNS du SAN. Ce **mappage faible** permettait l'usurpation d'identité (Certified, CVE-2022-26923, et variantes ESC). Depuis la mise à jour de mai 2022, les CA Enterprise ajoutent l'extension de sécurité SID aux certificats dont le sujet est construit depuis AD, et les DC exigent un mappage fort.

| Date             | Comportement des contrôleurs de domaine                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 10 mai 2022      | Publication de KB5014754 : mode compatibilité par défaut, événements d'avertissement pour les mappages faibles.                 |
| 11 février 2025  | Mode Full Enforcement par défaut ; retour au mode compatibilité encore possible via la clé StrongCertificateBindingEnforcement. |
| 9 septembre 2025 | La clé de registre n'est plus lue : le mappage fort est obligatoire, sans exception.                                            |

Un certificat est fortement mappé si l'une des conditions suivantes est vraie :

- il contient l'extension SID (OID 1.3.6.1.4.1.311.25.2) correspondant au compte ;
- il contient le SID dans le SAN sous forme d'URI (`tag:microsoft.com,2022-09-14:sid:<SID>`) ;

- le compte possède un mappage explicite fort dans `altSecurityIdentities` : `X509IssuerSerialNumber`, `X509SKI` ou `X509SHA1PublicKey`.

Les formats `X509IssuerSubject`, `X509SubjectOnly` et `X509RFC822` sont faibles. Les certificats émis hors ligne (sujet fourni dans la demande, NDES, CA tierce) n'ont pas d'extension SID : ils doivent recevoir un mappage explicite ou le SID dans le SAN. Les échecs sont journalisés par le KDC (journal Système, événements 39, 40 et 41).

## 18. Sécurité offensive AD CS : les vecteurs ESC

Depuis la publication « Certified Pre-Owned » (SpecterOps, 2021), les mauvaises configurations AD CS sont classées sous les identifiants ESC. Elles permettent souvent de passer d'un compte standard à Domain Admin, et une persistance par certificat survit à un changement de mot de passe. La figure illustre le vecteur le plus courant, ESC1, et les contrôles qui le neutralisent.

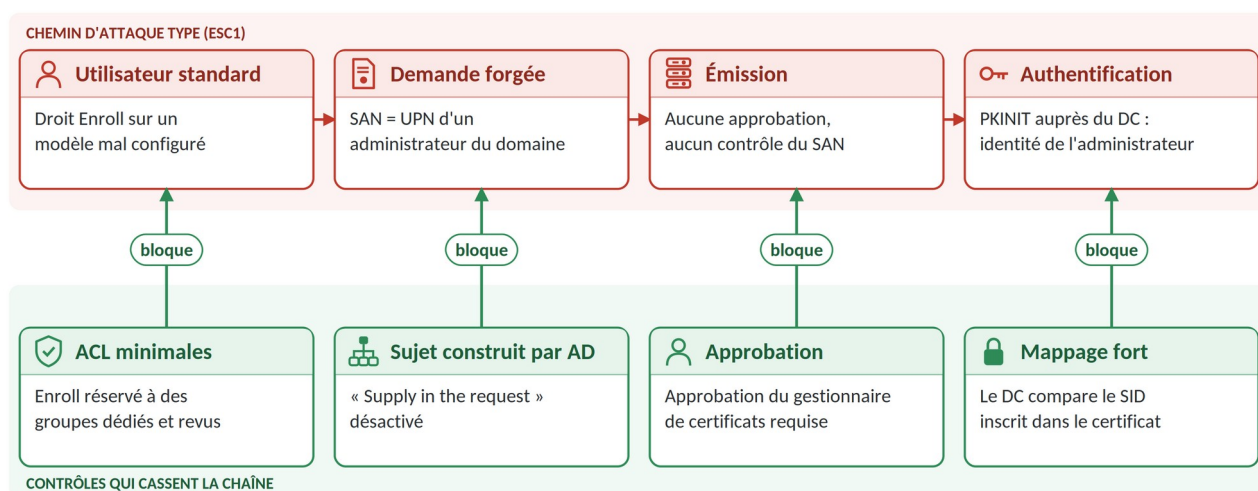


Figure 12 — Chemin d'attaque ESC1 et contrôles de défense

| Vecteur | Condition exploitable                                                                      | Contre-mesure                                                                |
|---------|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| ESC1    | Sujet fourni dans la demande + EKU d'authentification + enrôlement large sans approbation. | Construire le sujet depuis AD, ou exiger l'approbation ; restreindre Enroll. |
| ESC2    | Modèle « Any Purpose » ou sans EKU, ouvert à l'enrôlement.                                 | EKU explicites et minimaux.                                                  |
| ESC3    | Modèle Certificate Request Agent accessible (demande au nom d'autrui).                     | Restreindre l'agent ; restrictions d'agents d'inscription sur la CA.         |
| ESC4    | Droits d'écriture sur un modèle (WriteDacl, WriteOwner, WriteProperty).                    | Revue des ACL et des propriétaires des modèles.                              |
| ESC5    | ACL faibles sur les objets PKI d'AD ou le serveur CA.                                      | Traiter la PKI comme Tier 0.                                                 |
| ESC6    | Indicateur EDITF_ATTRIBUTESUBJECTALTNAME2 actif sur la CA.                                 | Désactiver l'indicateur (voir commande ci-dessous).                          |
| ESC7    | Droits ManageCA ou ManageCertificates trop larges.                                         | Réserver ces rôles aux administrateurs PKI.                                  |
| ESC8    | Relais NTLM vers Web Enrollment ou CES en HTTP.                                            | Supprimer Web Enrollment ; sinon HTTPS + EPA, NTLM désactivé.                |
| ESC9    | Modèle avec CT_FLAG_NO_SECURITY_EXTENSION (pas d'extension SID).                           | Retirer l'indicateur ; mappage fort.                                         |
| ESC10   | Mappage faible configuré dans le registre (Schannel, KDC).                                 | Paramètres par défaut, mappage fort.                                         |

| Vecteur | Condition exploitable                                                  | Contre-mesure                                         |
|---------|------------------------------------------------------------------------|-------------------------------------------------------|
| ESC11   | Relais NTLM vers l'interface RPC de la CA sans chiffrement exigé.      | Conserver IF_ENFORCEENCRYPTICERTREQUEST actif.        |
| ESC12   | Secret d'accès au HSM de la CA lisible sur le serveur.                 | Protéger le HSM et limiter l'accès local à la CA.     |
| ESC13   | Politique d'émission liée à un groupe AD (msDS-OIDToGroupLink).        | Auditer et restreindre ces liens.                     |
| ESC14   | Mappage explicite faible ou attribut altSecurityIdentities modifiable. | Formats forts ; ACL sur l'attribut.                   |
| ESC15   | Modèles v1 acceptant des Application Policies (CVE-2024-49019).        | Correctif de novembre 2024 ; dupliquer en v2 ou plus. |
| ESC16   | Extension SID désactivée au niveau de la CA (DisableExtensionList).    | Ne jamais désactiver l'OID 1.3.6.1.4.1.311.25.2.      |

```
# Vérifier / désactiver ESC6 sur la CA
certutil -getreg policy\EditFlags
certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2
Restart-Service certsvc
```

Pour l'audit, les outils open source **Locksmith**, **PSPKIAudit** ou le mode d'énumération de **Certipy** détectent la plupart de ces configurations ; Microsoft Defender for Identity propose des évaluations de posture AD CS lorsque son capteur est installé sur les serveurs CA. Ces outils ne doivent être utilisés que dans un cadre autorisé.

## 19. Magasins de certificats Windows

| Magasin                                | Usage typique                                                  |
|----------------------------------------|----------------------------------------------------------------|
| Local Computer\Personal (My)           | Certificats et clés privées de la machine et des services.     |
| Current User\Personal (My)             | Certificats de l'utilisateur.                                  |
| Trusted Root Certification Authorities | Racines explicitement approuvées.                              |
| Intermediate Certification Authorities | CA intermédiaires et CRL associées.                            |
| Enterprise NTAAuth (AD)                | CA autorisées à émettre des certificats d'authentification AD. |
| Untrusted Certificates                 | Certificats explicitement refusés.                             |

```
Get-ChildItem Cert:\LocalMachine\My      # certificats ordinateur
Get-ChildItem Cert:\LocalMachine\Root   # racines approuvées
certutil -store my                      # détail d'un magasin
certutil -verify -urlfetch certificat.cer # chaîne et URL de révocation
```

## 20. Feuille de route de déploiement

1. Définir les cas d'usage : TLS, 802.1X, VPN, contrôleurs de domaine, utilisateurs, S/MIME, équipements.
2. Rédiger la politique de certification : responsabilités, durées, algorithmes, révocation, sauvegarde, audit.
3. Concevoir les noms des CA et les URL AIA/CDP avant l'émission du premier certificat.
4. Construire la Root CA hors ligne ; protéger sa clé privée et ses supports.
5. Publier le certificat racine et sa CRL (HTTP et AD).

6. Installer une ou plusieurs Enterprise Issuing CA jointes au domaine, avec LoadDefaultTemplates=0.
7. Faire signer les certificats des CA d'émission par la racine.
8. Configurer AIA/CDP, la publication HTTP et, si besoin, l'OCSP ; tester depuis chaque zone réseau.
9. Créer des groupes AD dédiés aux populations d'enrôlement.
10. Dupliquer et durcir les modèles nécessaires ; retirer les droits trop larges.
11. Publier uniquement les modèles nécessaires sur les CA d'émission.
12. Créer les GPO d'auto-enrôlement ciblées.
13. Déployer NDES, CEP/CES selon les besoins ; ne pas installer Web Enrollment.
14. Activer l'audit AD CS, la supervision, la sauvegarde et les procédures de renouvellement.
15. Auditer la configuration (vecteurs ESC, mappage fort) avant la mise en production.
16. Tester émission, chaîne, révocation, expiration, renouvellement et scénarios de panne.

## 21. Ports et dépendances réseau

| Flux              | Port                  | Usage                                                                       |
|-------------------|-----------------------|-----------------------------------------------------------------------------|
| DNS               | 53 TCP/UDP            | Résolution des DC, des CA et des URL PKI.                                   |
| Kerberos          | 88 TCP/UDP            | Authentification des demandes et PKINIT.                                    |
| LDAP / LDAPS / GC | 389, 636, 3268        | Lecture des modèles, des ACL et du conteneur Public Key Services.           |
| SMB               | 445 TCP               | GPO (SYSVOL) et publication vers le partage PKI.                            |
| RPC / DCOM        | 135 TCP + 49152-65535 | Enrôlement et administration de la CA (MS-WCCE, MS-ICPR).                   |
| HTTP              | 80 TCP                | AIA, CDP, OCSP, SCEP (NDES).                                                |
| HTTPS             | 443 TCP               | CEP/CES, administration NDES.                                               |
| NTP               | 123 UDP               | Heure cohérente, indispensable à Kerberos et à la validité des certificats. |

## 22. Sécurité de la PKI

- Classer les CA, leurs sauvegardes, le partage de publication et les comptes d'administration PKI en **Tier 0**.
- Protéger la clé de la Root CA ; garder la racine hors ligne et documenter chaque cérémonie.
- Administrer les CA depuis des postes d'administration dédiés, avec des comptes distincts.
- Séparer les rôles (administrateur CA, gestionnaire de certificats, auditeur) lorsque l'organisation le permet.
- Utiliser des groupes AD dédiés pour Enroll et Autoenroll ; auditer régulièrement les ACL des modèles et des objets PKI.
- Rendre les clés privées non exportables sauf justification documentée.
- Supprimer CA Web Enrollment ; imposer HTTPS et EPA sur les services web d'enrôlement restants.
- Surveiller les modifications de modèles, de configuration de la CA et les émissions anormales.
- Maintenir CRL, AIA et OCSP disponibles : une révocation inaccessible provoque des pannes applicatives.
- Planifier le renouvellement des certificats de CA longtemps avant leur expiration.
- Désactiver les algorithmes faibles (SHA-1, RSA < 2048) et utiliser un HSM lorsque le risque le justifie.

## 23. Risques classiques et erreurs de conception

| Erreur                                              | Impact possible                                                                       |
|-----------------------------------------------------|---------------------------------------------------------------------------------------|
| Root CA en ligne en permanence                      | Exposition accrue de la clé racine.                                                   |
| URL AIA/CDP en HTTPS ou en LDAP seul                | Validation impossible hors domaine ou boucle de vérification.                         |
| Modèles trop permissifs                             | Émission de certificats d'authentification à des identités non prévues (ESC1 à ESC4). |
| Web Enrollment en HTTP                              | Relais NTLM et compromission du domaine (ESC8).                                       |
| CRL expirée ou URL inaccessible                     | Échecs de validation et incidents applicatifs généralisés.                            |
| Certificats de trop longue durée                    | Fenêtre d'exposition plus importante en cas de compromission.                         |
| Clés privées exportables partout                    | Copie et usurpation d'identité.                                                       |
| Pas de supervision des expirations                  | Pannes brutales de TLS, VPN, Wi-Fi ou d'authentification.                             |
| Renouvellement de CA non planifié                   | Rupture de la chaîne de confiance.                                                    |
| Suppression de certificats « anciens » sans analyse | Rupture d'un service encore lié à l'empreinte.                                        |

## 24. Exploitation et supervision

- Inventorier régulièrement les certificats émis, expirant et révoqués.
- Superviser l'expiration des certificats de CA, des CRL (NextUpdate), des certificats OCSP Signing et des certificats RA NDES.
- Tester périodiquement les URL AIA/CDP et les réponses OCSP depuis chaque zone.
- Conserver une procédure documentée de révocation d'urgence et de compromission de CA.
- Sauvegarder la base CA, la configuration, le registre et la clé privée ; tester la restauration dans un environnement isolé.

L'audit AD CS doit être activé à deux niveaux : sur la CA et dans la stratégie d'audit.

```
certutil -setreg CA\AuditFilter 127
auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
Restart-Service certsvc
```

| Événement          | Signification                                                              |
|--------------------|----------------------------------------------------------------------------|
| 4886 / 4887        | Demande reçue / certificat émis.                                           |
| 4888 / 4889        | Demande refusée / mise en attente.                                         |
| 4870               | Certificat révoqué.                                                        |
| 4882 / 4890        | Permissions de la CA / paramètres du gestionnaire de certificats modifiés. |
| 4898 / 4899 / 4900 | Modèle chargé / modèle modifié / sécurité d'un modèle modifiée.            |

```
certsrv.msc      # autorité de certification
certtmpl.msc     # modèles de certificats
pkiview.msc      # état Enterprise PKI (AIA, CDP, expirations)
certlm.msc       # certificats ordinateur
certmgr.msc      # certificats utilisateur
```

```
gpresult /h C:\Temp\gpresult.html
```

## 25. Diagnostic : un certificat TLS n'est pas accepté

1. Vérifier la date et l'heure du client et du serveur.
2. Vérifier que le certificat n'est pas expiré et que le serveur possède la clé privée.
3. Vérifier que le nom utilisé par le client figure dans le SAN.
4. Vérifier l'EKU Server Authentication.
5. Construire la chaîne jusqu'à une racine approuvée (certificat intermédiaire présent ou récupérable via AIA).
6. Tester AIA, CDP et OCSP depuis le client réel : `certutil -verify -urlfetch`.
7. Vérifier que l'application utilise le certificat attendu (liaison, empreinte).
8. Vérifier la compatibilité des algorithmes, tailles de clé et versions TLS.
9. Activer et examiner le journal CAPI2 : `wevtutil sl Microsoft-Windows-CAPI2/Operational /e:true`.

## 26. Cycle de vie complet

Un certificat suit un cycle continu : conçu à travers un modèle, il est demandé, émis, déployé puis utilisé ; la supervision déclenche son renouvellement avant expiration. Il en sort par révocation ou expiration, puis est retiré et archivé.

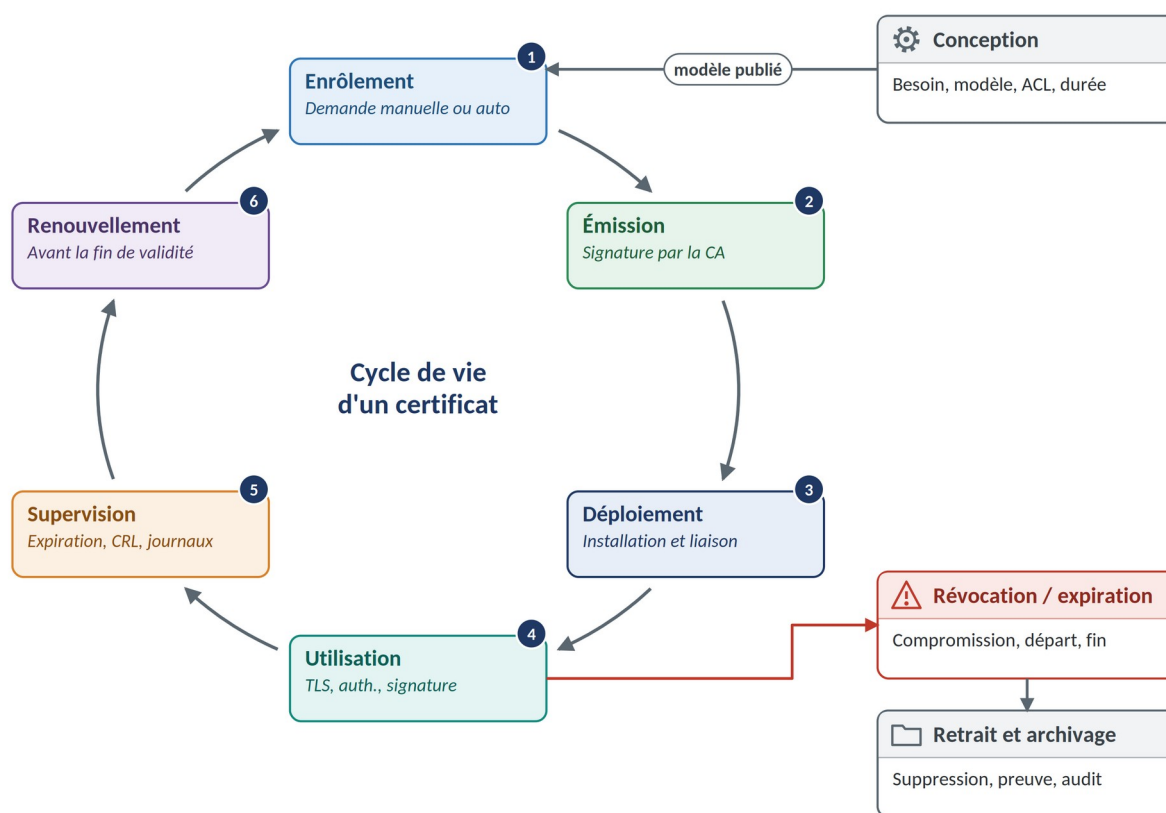


Figure 13 — Cycle de vie d'un certificat

## 27. Exemple de matrice de modèles

| Modèle             | Cible                  | EKU principal                                    | Déploiement                 | Durée*      |
|--------------------|------------------------|--------------------------------------------------|-----------------------------|-------------|
| Corp-Computer-Auth | Postes du domaine      | Client Authentication                            | Autoenroll GPO              | 1 an        |
| Corp-Server-TLS    | Serveurs ciblés        | Server Authentication                            | Autoenroll groupe dédié     | 1 an        |
| Corp-DC-Kerberos   | Contrôleurs de domaine | KDC Auth., Server/Client Auth., Smart Card Logon | Autoenroll GPO DC           | 1 an        |
| Corp-NPS           | Serveurs NPS/RADIUS    | Server Authentication                            | Autoenroll groupe NPS       | 1 an        |
| Corp-User-SMIME    | Utilisateurs autorisés | Secure Email                                     | Autoenroll                  | 1 an        |
| Corp-CodeSigning   | Développeurs approuvés | Code Signing                                     | Enrôlement avec approbation | 6 à 12 mois |

\* Valeurs de conception à adapter aux exigences de sécurité, de conformité et aux capacités de renouvellement.

## 28. Cryptographie moderne et post-quantique

Windows Server 2025 apporte à AD CS la prise en charge de **ML-DSA** (FIPS 204), algorithme de signature post-quantique normalisé par le NIST, dans ses trois jeux de paramètres (ML-DSA-44, 65 et 87). Les CA, les modèles et les réponds OSCP peuvent l'utiliser pour signer.

- Serveurs AD CS : Windows Server 2025 avec la mise à jour de sécurité de mai 2026 (KB5087539) ou ultérieure.
- Clients : Windows 11 24H2 ou 25H2 avec la mise à jour d'octobre 2025 (KB5067036) ou ultérieure.
- Aucune migration en place : une hiérarchie ML-DSA est une nouvelle racine et de nouvelles CA, validées en parallèle de la production.
- ML-DSA ne sert qu'à la signature : les modèles doivent utiliser un KSP CNG et l'objectif Signature, sans chiffrement ni échange de clé.
- ML-KEM et les certificats composites (classique + post-quantique) sont annoncés pour une phase ultérieure.

La compatibilité des applications et des équipements tiers reste le facteur limitant : l'adoption se planifie par un inventaire cryptographique et des tests pilotes.

## 29. Checklist de recette avant production

- ☐ Chaîne Root → Issuing CA valide depuis tous les segments réseau.
- ☐ Certificat racine distribué aux postes et serveurs concernés ; NTAUTH vérifié.
- ☐ AIA et CDP accessibles en HTTP ; contenus non expirés (pkiview.msc sans erreur).
- ☐ CRL de la racine et des CA d'émission publiées ; date de republication de la CRL racine planifiée.
- ☐ Modèles documentés, ACL revues, propriétaires connus ; aucun modèle par défaut inutile publié.
- ☐ Auto-enrôlement limité aux groupes et OU prévus.
- ☐ Un certificat de test s'émet, se renouvelle et, une fois révoqué, est détecté comme révoqué.
- ☐ Les applications TLS valident SAN, ECU, chaîne et révocation.
- ☐ Mappage fort vérifié : aucun événement KDC 39, 40 ou 41.
- ☐ Audit ESC réalisé (Locksmith, PSPKIAudit ou équivalent) sans constat critique ; EDITF\_ATTRIBUTESUBJECTALTNAME2 désactivé.
- ☐ Web Enrollment absent ; services web restants en HTTPS avec EPA.
- ☐ Sauvegarde de la CA réalisée et restauration testée.
- ☐ Alertes d'expiration configurées (CA, CRL, OCSP, RA NDES, certificats de service).

- ☐ Procédures de compromission de clé de CA et de certificat final documentées.
- ☐ Comptes d'administration et accès aux serveurs CA durcis (Tier 0) ; audit AD CS actif.

## 30. Références

**Vue d'ensemble AD CS :** <https://learn.microsoft.com/windows-server/identity/ad-cs/active-directory-certificate-services-overview>

**Documentation AD CS :** <https://learn.microsoft.com/windows-server/identity/ad-cs/>

**Certificate templates concepts :** <https://learn.microsoft.com/windows-server/identity/ad-cs/certificate-template-concepts>

**Manage certificate templates :** <https://learn.microsoft.com/windows-server/identity/ad-cs/manage-certificate-templates>

**CA Web Enrollment :** <https://learn.microsoft.com/windows-server/identity/ad-cs/certificate-authority-web-enrollment>

**Network Device Enrollment Service :** <https://learn.microsoft.com/windows-server/identity/ad-cs/network-device-enrollment-service-overview>

**Certificate Enrollment Web Service :** <https://learn.microsoft.com/windows-server/identity/ad-cs/certificate-enrollment-web-service>

**Post-Quantum Cryptography in AD CS :** <https://learn.microsoft.com/windows-server/identity/ad-cs/post-quantum-cryptography-overview>

**ML-DSA support in AD CS :** <https://learn.microsoft.com/windows-server/identity/ad-cs/ml-dsa-overview>

**KB5014754 – Certificate-based authentication changes on Windows domain controllers :**  
<https://support.microsoft.com/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16>

**SpecterOps – Certified Pre-Owned: Abusing Active Directory Certificate Services (2021) :** publication de référence sur les vecteurs ESC.

## 31. Glossaire

| Terme         | Définition                                                                                                             |
|---------------|------------------------------------------------------------------------------------------------------------------------|
| AIA           | Authority Information Access : extension indiquant où récupérer le certificat de la CA émettrice et le répondeur OCSP. |
| CDP           | CRL Distribution Point : extension indiquant où récupérer la CRL.                                                      |
| CRL           | Certificate Revocation List : liste signée des certificats révoqués.                                                   |
| CSR / PKCS#10 | Demande de certificat contenant la clé publique, signée par la clé privée du demandeur.                                |
| EKU           | Enhanced Key Usage : usages applicatifs autorisés d'un certificat.                                                     |
| EPA           | Extended Protection for Authentication : liaison de l'authentification au canal TLS, contre le relais NTLM.            |
| HSM           | Hardware Security Module : équipement matériel de protection des clés.                                                 |
| KSP           | Key Storage Provider : fournisseur de stockage de clés CNG.                                                            |
| NTAuth        | Magasin AD des CA autorisées à émettre des certificats d'authentification.                                             |
| OCSP          | Online Certificate Status Protocol : interrogation de l'état d'un certificat précis.                                   |
| PKINIT        | Extension Kerberos permettant l'authentification initiale par certificat.                                              |
| SAN           | Subject Alternative Name : identités alternatives du certificat (DNS, UPN, URI...).                                    |
| SCEP          | Simple Certificate Enrollment Protocol, utilisé via NDES.                                                              |